U.S. ARMY

INFORMATION MANAGEMENT SUPPORT CENTER (IMCEN)

HQDA CLASSIFIED ENTERPRISE NETWORK (HCEN)

SECURITY PROCEDURES

14 October 1999

Table of Contents

1. SECURITY PROCEDURES – GENERAL

These procedures are issued by the Headquarters, Department of the Army (HQDA) Information Management Support Center (IMCEN). They stipulate the Information Systems Security (ISS) responsibilities of appointed security officers and personnel who use automated information systems (AIS) within the HQDA Classified HCEN (HCEN).

1.1 Purpose

The purpose of this procedure is to establish procedures and guidelines for security for individuals located in Room 1E607 and members of the HCEN.

1.2 Scope and Applicability

These procedures are applicable to all individuals, government and contractor, that are assigned to Room 1E607 and/or are members of the HCEN.

1.3 Responsibilities

The protection of sensitive information is the responsibility of each individual who has knowledge of the information, regardless of how it was obtained. Security regulations do not guarantee protection and cannot be written to cover all likely situations. Therefore, basic security principles, common sense, and a logical interpretation of the regulations must be applied. Collecting, obtaining, recording or removing for any personal use whatsoever any information or material that is classified or declared sensitive in the interest of national security is prohibited.

1.4 Personnel Security

(A) Requirement for SECRET Clearance: All personnel having access to the HCEN must possess a valid SECRET clearance. A SECRET clearance is mandated because the HCEN processes classified data; and it is necessary to ensure personnel security and surety.

(1) Military and civilian personnel will provide authentication of a valid SECRET clearance by their agency's security office.

(2) The OSA Security Office, through the appropriate COR, will make verification of a SECRET clearance for contractor personnel.

(B) Personnel Recruiting:

(1) All requests to hire individuals for employment within the IMCEN must specify a requirement of sensitivity level 2 in Block E of SF52 which mandates that anyone hired for that position must possess a valid DOD SECRET security clearance.

(2) All job descriptions for IMCEN personnel must state that handling of classified and sensitive data is required.

(C) Personnel Security Responsibilities:

(1) Each first-line supervisor within the IMCEN system has the responsibility to ensure that all their employees observe sound security/surety practices and protect classified and sensitive material accordingly. The first line supervisor of each employee has the responsibility to report to the ISSO any violations of security procedures or instances when security procedures or practices are unsound, weak, or unenforced.

(2) All supervisors will be familiar with the provisions of Paragraphs 4-3 through 405, AR 380-19.

(D) Access Roster: The security representative will maintain an access roster reflecting those personnel who have met the security clearance requirements for access to Room 1E607. Upon departure or termination of an individual, the ISSO will be notified.

(E) Security Indoctrination: Prior to being granted access to the Room 1E607 and all ACL open storage certified areas, all staff employees and contractor personnel will be presented with or read a briefing which will familiarize them with particular security features and responsibilities associated with Room 1E607. This briefing will include review of designated required reading material.

(F) Annual Briefing: Each staff employee and contractor will receive an annual updated security briefing each year prior to the renewal of their system user ID and password.

(G) Debriefing: Each user must report to the ISSO upon termination of employment or cessation of access to the HCEN so that system access can be terminated.

(H) Visitors:

(1) All visitors to the Room 1E607 will be escorted by properly cleared personnel and will not be left unattended in operational areas.

(2) Entry into 1E607 requires verification of security clearance status by the Assistant Physical Security Officer and the approval of the individual charged with the responsibility of the area.

(I) Maintenance: Maintenance personnel will be escorted and not left unattended in offices or operational areas. Resident and repetitive maintenance personnel may be added to the Room 1E607 Access Roster by the ISSO.

(J) Remote Site Operations Personnel: All personnel who operate, maintain, or install equipment connected to the Room 1E607 classified computer facility by communication lines will require verification of applicable security clearance.

(K) Classified Conferences/Meetings: Each officer scheduling a classified conference in Room 1E607 is responsible for insuring that only personnel who have a need-to-know and are properly cleared are admitted to the conference area. A member of the

sponsoring element will closely monitor access to areas where classified conferences are in progress.

1.5 PHYSICAL SECURITY

IMCEN has daily physical security requirements that must be met to preclude unauthorized access to classified information or loss of government property.

(A) Building Passes:

(1) Everyone entering the Pentagon is required to have a Pentagon building pass (badge) or be escorted by someone who does. Military personnel may use their ID during normal duty hours. The badge must be shown to the guard upon entering the building and upon exiting, after 1800 hours.

(2) Requests for DOD building passes, by contractor personnel, with justification, are to be submitted through the appropriate COR to the IMCEN Administrative Officer.

(3) Building passes shall be worn visibly displayed on outer clothing at all times when in the restricted areas controlled by IMCEN.

(4) Passes issued for access to DOD buildings do not automatically grant access to Room 1E607.

(5) A favorable National Agency Check (NAC) is required before a permanent building pass can be issued. A temporary pass can be issued if a NAC has been initiated except for contractors. Temporary, or interim clearances cannot be granted to contractors.

(B) Property Passes: A property pass is required to remove any government-owned equipment from the Pentagon. An Optional Form 7 will be used. After completing items 1through 6, the form will be signed by the IMCEN Property Manager in room 1E607. The DOD guard will collect the pass upon departing the building with the equipment. The IMCEN site manager must be notified prior to the removal of any office equipment or property.

(C) Lock & Key Control:

(1) A security representative will change the combination to a safe or door lock whenever someone who has had access no longer requires it or, at a minimum, every 6 months. The mechanical cypher lock on 1E607 are stored with the combinations (Standard Form 700) in Safe 1, Room 1D659. The instruction manuals for changing the combinations are also stored here.

(2) The keys for the furniture, i.e., the desk drawers, cabinets, etc. have been issued to the equipment's owner. There are no door keys in use; only the combination locks. Combinations are given out only by security representatives

(3) All doors allowing access to IMCEN-occupied spaces will be secured by appropriate locks or locking devices. All locks and keys for all office doors will be strictly controlled and accounted for.

(4) The IMCEN Administrative Officer will maintain a central Key Control Register (DA Form 5013-R).

(a) Keys will not be duplicated.

(b) Individuals will receipt for and be held accountable for proper use and safeguarding of keys issued to them.

(5) A semi-annual inventory will be made using DA Form 5014-R, Activity Lock and Key Control Semi-Annual Inventory Record.

(6) Individuals must report lost or stolen keys promptly to the Physical Security Officer. Keys lost through carelessness or neglect may result in disciplinary action and/or corrective action designed to maintain the integrity of the key lock system.

(D) Restricted Access/Discussions:

(1) Do not discuss classified information with any individual unless the individual's clearance has been verified and the individual has a valid need-to-know. Additionally, classified conversations should only be conducted in restricted areas where there is no potential for overhearing classified conversations.

(2) Classified information should never be discussed over unsecured phones. If there is a valid need to discuss classified information over the phone, arrangements should be made to use the secure telephone unit (STU-III) located in the OCSA security manager's office or the "gray" phone located in the Special Security Office (SSO).

(3) **Computer Vault:**

(a) The vault is a restricted access area approved for storage and discussion of information classified up to SECRET. Access is restricted to those who have a SECRET clearance and a need to work with our data or systems. Unrestricted access will only be granted to IMCEN personnel who have the requisite clearance and a need to work in a secure area. The director may grant other personnel unrestricted access if they have the requisite clearance and a need for continual use of the secure computing equipment.

(b) Uncleared personnel requiring access to the vault must be escorted by cleared personnel. The escort will ensure that classified material is secured prior to permitting an uncleared visitor entry to the vault.

(c) A visitor's log of all visitors viewing classified material and demonstrations in the computer vault will be maintained by the offices presenting the material or demonstration. This visitor's log will be kept in the vault demo room. Site administration personnel will maintain a log (or some other sort of record) of all computer maintenance performed in the vault. Logging visitors who are escorted and conducting unclassified business is not required.

(d) Security alarm technicians perform monthly maintenance checks on the vault alarm. Alarm technicians are civilian contract personnel who work for Defense Protective Service (DPS). Verification of authorization can be made by contacting DPS, 697-1001.

(e) A security representative controls the cypher and Sargent & Greenleaf lock combinations to the computer vault. To lock/unlock the vault, a personal identification code (PIC) is needed to activate/deactivate the alarm. A PIC will be issued to those who work in the vault. The security representative receives PICs from DPS Security, as needed. To unlock the vault: unlock the S&G lock and punch in the cypher combination. You will then have about 20 to 30 seconds to turn on the lights and deactivate the alarm. To deactivate the alarm (place it in access mode), simply punch in the PIN number followed by the access key. The computer displays "Set to Access" followed by "ACU Ready." Don't forget to annotate SF 702 when unlocking the vault. To secure the vault, shut off all desk and office lights. Next, stand still and wait for the "Alarm" red light to go out. The other two lights, "Set" and "Data Link" should be green. Punch in the PIN followed by "GO/F1." The computer displays "Set to Secure." You then have about 20 to 30 seconds to shut off the main bank of lights and depart the vault. Wait about 30 seconds; if the alarm was successfully activated, a steady alarm tone that lasts about 3 to 5 seconds will be heard. Lock the S&G lock by spinning the dial 4 or more times, then check to ensure the vault is secure by entering the cypher lock and pushing the door. Annotate SF 702. If a 3-to-5-second steady tone is not heard, the alarm was not properly set. You must then reset the alarm to access mode, and then retry setting it to secure mode. Note that instructions for activating and deactivating the alarm are posted near the system. If difficulty is experienced with the system, call DPS Security; the number is also posted near the system.

(E) DPS Alarm System: The computer vault intrusion detection system is the state-of-the-art computerized system that terminates at DPS, 697-1001. The alarm is a silent alarm

which means that when triggered it is only heard in DPS. The alarm system consists of four zones: (1) a 24-hour magnetic contact detector switch on the secondary vault entrance; (2) a 24-hour magnetic contact detector switch on the door leading to a disconnected boiler in the left upper area; (3) a magnetic contact detector switch on the main vault door; and (4) wall-mounted ultrasonic motion detectors throughout the vault. Note that the old motion detection sensors (small ceiling-mounted cylinders that look like the smoke detectors, except the old detection sensors have no red indicator light) are no longer connected.

1.6 ADP SECURITY

(F) **Data:** Remember that computer security means two things, prevention of unauthorized disclosure of data and prevention of unauthorized destruction of data. So, whether processing classified or unclassified data, use the security software that has been provided by the site manager. See the site manager for a copy of the security software and/or instructions for its use.

(G) **Mandatory:** The contents of this manual are intended to support and conform to the following basic DOD ADP system security policies:

(1) **Individual Accountability.** Each user's identity will be positively established on the HCEN.

(2) **Environmental Control.** The ADP system will be externally protected to minimize the likelihood of unauthorized access to system entry points, access to classified information in the system, or damage to the system.

(3) **System Stability.** All elements or components of the ADP system will function in a cohesive, identifiable, predictable, and reliable manner in that malfunctions are detected and reported within a known time.

(4) **Data Integrity.** Each file or collection of data in the ADP system will have an identifiable origin and use. Its accessibility, maintenance, movement, and disposition shall be governed on the basis of security classification and need-to-know.

(5) **System Reliability.** The system should function so that each user has access to all of the information to which he is entitled, but no more.

(6) **Communications Links.** These links and lines will be secured in a manner appropriate for the material designated for transmission trough such lines or links. (See AR 380-51 for guidance and policy concerning the transmission of official information).

(7) **Classified and Sensitive Unclassified Material.** Such material handled and produced by the ADP system or stored in or on media will be safeguarded as appropriate for the classification or sensitivity assigned.

(H) Hardware Acquisition: The provisions of Chapter 7, AR 380-19, must be considered during the development of requirements for hardware. The specification for any hardware acquisition will be submitted to the ISSO for a security review prior to release to the contracting office.

(I) Room 1E607: Ensure that the site manager is notified before moving or removing any equipment in or from the vault.

(J) Accreditation:

(1) Any site with a processor that has been accredited IAW Chapter 11, AR 380-19, and that desires to connect with the HCEN computer system will provide a copy of the Accreditation Document and Risk Analysis to the IMCEN ISSO.

(2) No changes will be made to the operating system or executive and no equipment will be installed until a determination has been made by the ISSO as to whether or not reaccredidation is required IAW paragraph 11-5c, AR 380-19.

(K) Procedures for Removable Hard Drives:

(1) **Accountability**. The OISSO for the classified computer with the hard drive will have control of the equipment. Computers used for the processing of classified information will be considered to be classified general-purpose personal computers and will be operated and protected according to the procedures delineated in AR380-5.

(2) **Procedure**. Computers located in areas that have NOT been designated as approved for “Open Storage” will use either laptops or desktop computers with removable hard drives when processing classified information. The procedures below will be followed in handling the classified removable hard drive.

(a) The removable hard drive used to process classified information will be clearly marked “SECRET” using SF 70 SECRET classification label.

(b) Only information up to and including the SECRET classification level will be processed and stored on the hard drive.

(c) When the classified hard drive is not being used in the designated PC, it will be locked in an approved security container just as classified documents and floppy disks are stored.

(d) At no time will the removable hard drive be left in the computer or anywhere other than the locked container without being under the direct control of a properly cleared member of the office.

1.7 Notebook Computer

(1) **Introduction**. This procedure will be used in the use and control of using laptop computers to process classified information. If a computer contains a non-removable hard disk that stores classified material, the entire computer must be stored in an GSA approved storage area at all times that the computer is not in the possession of the user.

(2) **Accountability**. The OISSO for the classified notebook computer/laptop will have control of the notebook. Laptops used for processing classified information will be considered to be classified general-purpose personal computers and will be operated and protected according to the procedures delineated in AR 380-5.

(3) **Procedure**.

(a) Laptops will be properly labeled to indicate the level of classified information they contain and the restriction on whom may use the computer, in accordance with AR 380-5. Laptops may be used in unsecured physical areas only if physical control of the computer can be strictly maintained at all times and visual access to the computer screen can be strictly limited to persons authorized to see the classified information.

(b) Persons transporting computers containing classified information must meet all the requirements and comply with all the regulations for transporting documents at the same level classification. A classified laptop and removable media containing classified information must be transported in a locked computer bag or other locked container. A classified laptop taken on TDY must be stored in GSA approved safes and other security containers. Classified laptops and classified removable media may not be left unattended in hotel rooms, office or automobiles, and cannot be stored in hotel safes or other non-secure, non-GSA standard containers.

1.8 Backups

(A) Purpose and Scope: This SOP defines the requirements and general guidelines for creating backups of network data. It also seeks to define a strategy for archiving backups. This section applies only to the HCEN. Other backup systems may be mentioned due to their relationship with ARDA II.

(B) Responsibilities:

(1) The primary ARDA II administrator is responsible for ARDA II backup procedures and execution of backups. The primary ARDA II administrator is also responsible for modifying this document as adjustments are made to the system.

(2) Other ARDA II administrators are responsible for notifying the primary administrator if they modify any of the backup configurations.

(C) Brief Definition: The backup system consists of several different hardware and software platforms for performing a snapshot copy of network data and server configurations. Incorporated into this system are tape drives, disk copies, diskettes, and repair disks.

(D) Design Goals:

(1) Dependability. All critical systems will receive regular backups through an automated system. The frequency of these backups will be such that a significant amount of data will never be lost should a system failure occur.

(2) Reliability. The ARDA II administrators are responsible for maintaining the reliability of the system. The primary administrator will review the procedures four times annually to verify system integrity.

(E) Design Requirements:

(1) The backups will be configured to minimize the time required to restore an entire system.

(2) The backup schedule will be automated and periodic backups initiated without user intervention.

(3) Backups will run through to completion without user intervention. A single backup job will require no more capacity than that which will fit on the storage device.

(4) The frequency of a complete backup will be no greater than one week.

(5) Each month a complete backup set will be set aside as an archive copy of the data that was backed up.

(6) Backup sets will not be collocated with the systems they backup. If the backup media is collocated, a fire and blast resistant container will be used as the storage location.

(7) Each backup set will be labeled appropriately as per the system that it is a backup for.

2. PRIVACY ACT PROCEDURES

2.1 General

All personnel have a special responsibility to protect personal data from unauthorized disclosure. Automated systems personnel, in the normal course of performing their assigned functions, have access to significant amounts of personal data. Irreparable damage can be done to an individual by disclosing or failing to adequately safeguard personal information relating to that individual. Therefore, personal information acquired in the work environment must be scrupulously safeguarded. Similarly, all personnel must be alert to, and protect against, unauthorized alterations of personal data.

(Nothing contained in this manual is to be used to contradict or is to be construed as authorizing a contradiction to any or all of the regulations pertaining to the Privacy Act or the Freedom of Information Act.)

2.2 Policy

It will be IMCEN's policy to:

(A) Protect the personal privacy of all individuals from unwarranted invasion.

(B) Permit an individual to know what records IMCEN has proponency for concerning him; to have access to, or copies of, such records or portions thereof; and to request amendment of such records whenever exemptions do not apply or there is no significant, legitimate governmental purpose to be served by claiming an exemption.

(C) Collect, maintain, use, or disclose any record or identifiable personal information only for a necessary and lawful purpose.

(D) Insure that all information is timely, relevant and accurate for the intended use and is adequately safeguarded to prevent misuse or unauthorized access/disclosure.

(E) Act on all requests for access to and amendment of records from individuals promptly, accurately, and fairly.

(F) Obtain from all proponents of systems not subject to the Privacy Act of 1974 as implemented, a signed statement to that effect prior to any processing by IMCEN.

(G) Insure that all proponents of systems of records have published a system notice in the Federal Register as required by AR 340-21 prior to any processing by IMCEN.

(H) Provide to Privacy Act input, output, and processing media at least the same degree of protection required for "FOR OFFICIAL USE ONLY" material (e.g., storage in locked cabinets).

(I) Never disclose individual home addresses or list or compilations of names and home addresses without the written consent of the individual(s) involved.

2.3 Responsibilities.

(A) All users must be familiar with the provisions of AR 340-21 and Appendix J, AR 380-19. Particular attention should be paid to the procedures specified in Paragraph J-4, AR 380-19. Software development and hardware acquisition must include as many safeguards as necessary and practical.

(B) System Proponents. See Paragraph J-3a, AR 380-19.

3. CONTINGENCY PLAN FOR ROOM 1E607

3.1 Purpose and Objectives

(A) The purpose of this contingency plan is to outline a formal plan of action to be followed in the event that the normal ADP environment is impaired or disrupted. The impairment or disruption can range from a few hours to several days depending on the cause or situation. This plan consists of planning, preparation, and action phases and will provide a plan of action for emergency and recovery operations.

(B) The objective of this contingency plan is to provide managers, operations personnel, and users of the Classified Backbone with procedures so that the required services can be carried on in a limited fashion and and that designated critical and priority jobs can be processed until full recovery can be achieved.

3.2 Scope

The scope and depth of the contingency plan is influenced by the activity's ADP environment, the criticality of the functional applications being supported, and the user's ADP support requirements. This plan covers Room 1E607 in the Pentagon.

(A) **Limited loss of ADP capability.** The impact will vary depending on the urgency or loss potential of individual tasks. Typical causes are:

- Failure of key communication circuits
- Failure of electric utilities
- Loss of key documentation
- Partial loss of air conditioning or power
- Non-availability of critical personnel
- Sudden expansion in workload due to a national emergency or some other critical event.

(B) **Interruption to ADP Operations.** The duration of the interruption will depend on the time needed to restore normal operations. All tasks are usually affected yet with minimal or no damage to the facility. Typical causes are:

- Failure of a major computer hardware unit or air conditioning unit
- Failure of electric utilities
- Fire, flood, or sabotage in the ADP operating environment
- Failure of the switch
- Intrusion of smoke, dirt, dust, or water
- Non-availability of operation personnel

(C) **Major Damage or Destruction of the Facility or Contents.** All operations would be affected. Backup operations and repair of the facility or contents would be required to restore normal operations. Typical causes would be:

- Natural acts (earthquake, flood, lightning, etc.)
- Civil disorders (bombing, explosions, fire, etc.)
- Mechanical breakdown (water pipe bursting, junction box fire)
- Catastrophic accidents (airline crash, chemical spills, etc.)
- International incident (war)

(D) **Responsibilities.** It is the responsibility of the ISSO, the NSO, and every individual to understand and follow this contingency plan.

3.3 Situations

(A) **Personal Injury or Illness:** One of the primary reasons that the "2-persons inside the computer room at all times" regulation is in effect is that if one person becomes disabled in any manner (through being accidentally electrocuted, bad reaction from prescribed medicine, etc.), the other person can administer and/or call for help.

(1) Call for assistance as soon as possible—only life saving and first aid procedures take precedence.

(2) Prevent further injury by removing the person to safety or eliminating hazardous condition, whichever would result in less trauma for the victim.

(3) In the case of electrocution, operate emergency power-off before attempting to touch the victim if they are still in proximity or in contact with the electrical source.

(4) If appropriate, administer CPR, stop arterial bleeding, execute Heimlich maneuver, or other immediate life saving treatment.

(5) Report incident: Call U.S. Army Clinic (695-1031)

(a) Notify FPS - GSA (697-5555)

(b) Notify ISSO – William Dugger (693-7070)

(6) Render assistance to victim(s) until arrival of paramedics:

(a) Make victim(s) as comfortable as possible

(b) Treat for shock

(c) Perform other first aid as appropriate

(B) Fire within the Room

(1) Report fire (call 697-5555 - notify Pentagon Occupant Emergency Organization Command Center - alternate: Federal Protective Service Operations Office at 697-4151 or GSA Building Manager's Office at 697-7351). Also notify Site Manager.

(2) Activate fire alarm box inside main computer rooms or others in the areas as guides for emergency service personnel to reach the scene.

(3) Assess life-safety hazard; evacuate facility if necessary.

(4) Initiate loss control procedures:

(a) Time permitting, secure classified processing.

(b) If fire involves electric power source/cable, use emergency power-off.

(c) If fire involves localized support equipment, terminate power to unit if possible, power down system gracefully. Extinguish fire in the equipment if possible.

(d) If fire involves documents, printer paper, and/or magnetic storage media or other concentrations of combustible material, attack fire as soon as practical; power down system gradually following apparent extinguishment; check material for re-ignition.

(5) Assist fire department firefighters upon arrival.

(6) Re-secure facility following completion of emergency service activity.

(C) Evacuation Due to Fire Elsewhere in Pentagon:

(1) Notify ISSO/Site Manager.

(2) Shut down system gracefully.

(3) Time permitting, secure classified material.

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(D) Evacuation Due to Hazardous Chemical Spill:

(1) Notify ISSO/Site Manager.

(2) Shut down system(s) gracefully.

(3) Time permitting, secure classified material.

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(E) Evacuation Due to Bomb Threat

(1) Notify ISSO/Site Manager.

(2) Shut down system(s) gracefully.

(3) Time permitting, secure classified material.

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(F) Evacuation Due to Rioting/Terrorist Actions on Pentagon Grounds:

(1) Notify ISSO/Site Manager.

(2) Shut down system(s) gracefully.

(3) Time permitting, secure/destroy classified material (see Section 2.3)

(4) Lock doors upon departure.

(5) Proceed to appropriate marshalling area via safest route.

(G) System Crash

(1) Evaluate console message(s).

(2) Isolate component(s) to minimize system disruption.

(3) Examine components to determine whether any damage occurred.

(4) Notify ISSO of system status and anticipated actions.

(5) Tag affected component(s) and log details of incident to facilitate subsequent corrective action.

(6) Download active files to secondary storage prior to system shutdown; be especially aware of securing classified data.

(7) ISSO will do the following:

(a) If system is still up, message to alert system users to specific degradation problem.

(b) Dispatch personnel to assist operator(s) in troubleshooting and restoring system, if possible.

(c) Contact appropriate entity to request necessary repairs (i.e., vendor's customer/field engineer, lead systems programmer, hardware technician, etc.).

(d) Post message to system users.

(H) ADP Equipment Damage:

(1) If needed, effect life safety measures immediately.

(2) Isolate and shut down unit(s) affected.

(3) Report condition to ISSO/Site Manager.

(4) Evaluate effect on system operation and take actions to minimize disruption.

(5) Locate articles that are evidence of equipment failure and establish safeguards to prevent their disturbance prior to investigation.

(I) Unscheduled Power Outage, Surge, or Other Electrical Irregularity:

(1) Following a system crash, inspect equipment for damage. If needed, request a thorough inspection and test by vendor Customer/Field Engineer(s) prior to restoring system on-line.

(2) When system remains on-line following a power fluctuation which contaminates the operating system or applications, bring the system down gracefully and perform a standard restart and recovery operation, paying particular attention to the classified side of the system.

Note: *When there is a potential for local extreme thunderstorm activity, systems should be shut down to prevent damage likely to result from power surges and blackouts as well as electromagnetic interference with transmission lines from lightning discharges. Systems shall be brought down gracefully prior to scheduled power outages.*

(J) Smoke or Excessive Dust in Main Computer Rooms:

(1) Notify ISSO/Site Manager.

(2) Shut down all equipment gracefully.

(3) Seal all IT media, including classified, in appropriate containers or remove from room.

(4) Seal door(s) edges with tape upon departure if possible and activate locks.

(5) Evacuate area when necessary.

(K) Excessive Heat/Humidity within Main Computer Room:

(1) Notify ISSO/Site Manager.

(2) Check HVAC (heating, ventilating, air conditioning) operations

(a) Air handling unit re-circulating fan running?

(b) Chill water temperatures satisfactory?

(c) Filters satisfactory?

(3) Check adjacent areas to determine if room temperatures outside the computer rooms are also excessive.

(4) When directed, shut down peripheral equipment to reduce heat load; also turn off fluorescent lighting if possible. (Temperature in excess of 80 degrees F or relative humidity greater than 65%.)

(5) Set up pedestal fan(s) to help cool CPU/disk drive cabinets

(6) Notify users to terminate sessions when temperature exceeds 83 degrees F.

(7) Shut down CPU and disk drives when temperature exceeds 85 degrees F or relative humidity exceeds 80%, making certain to secure classified processing.

(8) Have vendor's Customer/Field Engineers) examine and test IT equipment prior to restoring normal system use

(9) ISSO/Site Manager:

(a) Initiate trouble call to the GSA Pentagon Building Administrator (695-270).

(b) Contact Utility Systems Repair Operator (697-7351) to ascertain the status of climate control conditions for the sector(s) affected.

(c) If the prognosis for conditions in the immediate area surrounding computer room indicates continuing degraded climate control, instruct operator(s) to phase out peripheral and processing equipment, thereby minimizing potential damage.

(L) Insufficient Heat/Humidity within Main Computer Room:

(1) Check air handling unit for satisfactory operation.

(2) Notify ISSO/Site Manager when temperature drops below 65 degrees F, humidity drops below 45% or if static electricity is evident.

(3) If temperature continues to drop and adjacent rooms also exhibit insufficient heating during winter conditions, request instruction from ISSO.

(4) ISSO/Site Manager:

(a) Contact Utility System repair operator (697-7351) to ascertain the status of building climate control for the sector(s) affected.

(b) Initiate trouble call to restore local utility operation.

(c) Order system shut down when building conditions are expected to continue degrading as a result of utility failure.

Note: *Disk/tape drive misalignment is to be expected for read/write operations occurring at widely divergent temperatures--subsequent attempts to recover data are not likely to be successful unless performed under similar conditions.*

(M) Water Damage in Computer Room:

(1) Notify ISSO.

(2) Shut off source of leak, if possible.

(3) Terminate jobs in progress after posting a system warning message to users to conclude processing.

(4) Spin down and remove disk(s) from drive(s).

(5) Power down hardware and cover with plastic sheeting.

(6) Power down air conditioning equipment.

(7) Put tapes, disks, run books, and source documents in storage container(s) or remove from site.

(8) Stand by to provide access for utility repair crew. (Secure space when unattended.)

(9) Site Manager:

(a) Assess extent of service interruption (repair operations may result in loss of air conditioning for an extended period--significant moisture within the computer room may necessitate comprehensive computer system inspection and testing prior to restoring on-line service).

(b) Submit trouble call to Utility Systems Repair Operator (697-7351 or 695-7622).

(10) ISSO: Post message(s) to affected system(s) to advise users of conditions and of the probably duration of the outage.

(N) Physical Intrusion by Unauthorized Personnel:

(1) Notify Site Manager; providing enough detail to allow for adequate response.

(2) Advise intruder(s) of restricted status of space and ask intruder(s) to leave.

(3) Prepare to shut down system if potential for damage or compromise of classified data is indicated.

(4) If weapons are carried by intruder(s), do nothing to antagonize, but cooperate to the extent that system resources are not hazarded. Comply with demands if life safety is threatened.

(5) Note characteristics of intruder(s) to facilitate reporting after the incident.

(6) Assist Pentagon security personnel upon their arrival.

(O) Unauthorized System Access Attempt:

ISSO:

(1) Periodically, review Sun system audit trial to determine if any sources of impropriety exist. If found, request interception and notification of file owner.

(2) Initiate interactive system countermeasures to isolate activity of penetrator.

(P) Discovery of Physical Resource Tampering:

(1) Notify ISSO.

(2) Preserve evidence for subsequent investigations.

(3) Note conditions at the time of discovery.

(4) Prevent access by all personnel not directly involved with resolution of the incident.

(5) ISSO:

(a) Dispatch functional supervisor to the scene.

(b) Request investigative support of site and/or advisement of INSCOM/ACSI as necessary.

(c) Advice person(s) on scene of anticipated actions by respondents.

4. SECURITY OFFICERS/POINTS OF CONTACT

ISSM, Mr. Ronald L. Greenfield, Room 1E614, 695-7447

- Responsible for implementing the IMCEN's Security Plan

ISSO, Mr. William D. Dugger, Room 1D614, 695-7070

- Ensures newly assigned personnel are aware of security procedures
- Maintains applicable security publications
- Maintains the IMCEN Room 1E607 Security SOP
- Hardware/software acquisition
- Site administration
- Reviews contracts for security considerations
- Site accreditation
- Clears equipment for use in or removal from Room 1E607
- Maintains combinations and change keys to all locks

Hand Receipt Holder, SSG Ronald D. Hamilton, Room 1E629, 614-7769

- Computer equipment accountability

Security Manager, Ms. Luticia Hook, Room 1E600, 614-6928

- Assists ISSO with Accreditation
- Approves vault access for IMCEN personnel
- Maintains security clearance roster
- Maintains liaison with all other security representatives

SAIS-AI Security Manager, CPT Lisa Keller, Room 1D659, 614-6909

- Controls vault access
- Maintains clearance roster
- Maintains applicable security publications
- Changes and issues combinations and PIN numbers
- Maintains liaison with all other security representatives
- Coordinates locksmith and building manager support

Security Representative, Mr. Dennis T. Kamihara, Room 1E607, 614-9277

- On-site IMCEN representative for Room 1E607

- Assists ISSM/ISSO with Accreditation
- Network security
- DPS security liaison
- Maintains liaison with all other security representatives
- Coordinates building manager support

IMCEN Property Management Officer: LTC Dean E. Mattson, Room 1D600, 697-1365

- Property pass authorizations

Defense Protective Service (Lockeed Martin, Greg Milewski, 697-1007)

- Cognizant security office for vault operations
- Monitor and respond to vault alarm system
- Maintain combination and cipher override key
- Provide PIN numbers for alarm access
- Point-of-contact for alarm technicians

Administration Office, Luticia Hook, Room 1E600, 695-9693

- Initiates security investigations
- Property pass authorizations
- Request locksmith support
- Request building repairs or alterations
- Requests building passes (badges)
- Maintains master clearance roster
- Provides courier orders

SAM Directorate of Security, Mike Covert, Rosslyn Plaza North, 588-6589

- Provides guidance and assistance with accreditation
- Approves accreditation

Safety, Security Support Services - Wash, Dennis Thomidis, 602-3895

- Provides inspection and approval for open storage

DCSINT Automation Security Officer: Unknown, Room 2D481, 697-7373

- Provides technical automation security information

HQDA Special Security Officer (SSO): Unknown, Room 2A474, 695-2758/6663

- SCI indoctrination

- SCI courier orders
- SCI visit certifications
- Armed Forces Courier Service
- DSSCS communications
- Daily Black Book
- SCI Research Facility

Pentagon Building Manager: Mrs. Jan O'Neil, Room 1A327, 697-7351

- Maintains office blueprints
- Handles requests for common area maintenance
- Performs periodic fire extinguisher inspections

Pentagon Building Pass Office: Room 2E170A, 695-5923

- Issue building passes (badges)

Pentagon Safety Office: Mr. Gilson, Room 2D533, 693-3684

- Liaison with fire engineers
- Federal Protective Service Office: Room 1A313, 697-4151
- Lost & found property

5. CERTIFICATION AND ACCREDITATION (C&A)

Certification is the technical evaluation that establishes the extent to which a particular computer system meets a pre-specified set of security requirements for use in a particular environment. The Certifying Official makes a recommendation for or against accreditation based on this evaluation.

Accreditation is a formal declaration by the Single Agency Manager (SAM) Designated Approving Authority (DAA) that an information system or network is approved to operate:

- In a particular security mode
- With a prescribed set of countermeasures
- Against a defined threat and with stated vulnerabilities and countermeasures
- Within a given operational concept and environment
- With stated interconnections to other information systems
- With an appropriate level of protection (level of risk) for which the DAA has formally assumed responsibility
- For a specified period of time

In approving a system for operation, the DAA formally accepts responsibility for the security of the system and declares that the system will provide an appropriate level of protection against compromise, destruction, or unauthorized modification of data when operated under the conditions stated in the accreditation.

Certification and accreditation of systems must be accomplished separately for each level of overall system classification. Systems accredited by SAM will fall into one of four categories: Unclassified/SBU; Confidential; Secret; or Top Secret**.**

5.1 Explanation of Requirements

(A) **All** DOD automated information systems (including networks and stand-alone computers) must be accredited **prior to being placed in service**.

(B) Agencies seeking accreditation must address a request for accreditation to the organization's ISSM, who evaluates the request and forwards his/her recommendation to the DAA (see Section 5.2, C&A Documentation Requirements).

(C) **Reaccredidation:**

(1) A system must be reaccredited every three years, at a minimum. The Certifying Official should start the reaccredidation process at least three months prior to the

end of the current accreditation. This will provide an overlap in the accreditations and help ensure that the accreditation of the system will not lapse for any period of time.

(2) Reaccredidation is also required as a result of significant changes to the system configuration, operation, or environment. Some examples of changes that would require reaccredidation:

(a) Increase in sensitivity level, e.g., a change from classified sensitive level 3 to classified level 2.

(b) Replacement or modification of the main computer/major system. (Not applicable to operation of small computers (e.g., PCs, laptops, notebooks).

(c) A change in the security processing mode to a more complex mode.

(d) A major change to the operating system, or executive software. (Not applicable to operation of small computers.

(e) A change in the physical environment. Only if the change would introduce new threats and vulnerabilities that would require reassessment under the risk management program.

(f) Any situation that would cause the initial or previously established accreditation to become invalid, for example, newly discovered system insecurities.

(D) **Accreditation Amendment.** When a minor change is made to an accredited AIS, such as the addition of a workstation, an amendment is required. The agency will address a request for an amendment to the ISSM, who will evaluate the request and forward his/her recommendation to the DAA.

(E) **Certifying Official.** The Certifying Official is usually the organization's ISSM. The ISSM establishes and administers the organization's ISSP and is responsible for obtaining accreditation for information systems under the organization's control. ISSMs are appointed by their commanders, agency chiefs, directorate chiefs, or managers of the activities operating the information system. The Certifying Official will prepare or oversee the preparation of the certification package.

In the case of large or complex systems, the Certifying Official may appoint a Certifying Team to assist with the certification process.

(F) **Certification and Accreditation of Networked Systems.** If possible, networks will be certified and accredited as a whole. Any subnet not included in the certification and accreditation (C&A) of the network must be certified and accredited separately.

(G) **Interim Accreditation.** Normally, all certification tasks must be completed before the Certifying Official requests accreditation from the DAA. However, the DAA may grant

interim accreditation when a mission-critical system must be operational before all the required certification tasks are completed. In this case, the Certifying Official must document the residual risks that result from the unfinished certification tasks. The DAA will decide whether he or she is willing to accept the additional risks and AIS Accreditation is defined as the official approval to operate a computer system at a designated level of sensitivity. Formulation of the accreditation documentation is a responsibility of the ISSO. The accreditation process must be completed prior to acquiring a system.

5.2 C&A Documentation Requirements

The following paragraphs explain all of the documentation requirements for HQDA agencies seeking accreditation by IMCEN to operate an AIS within the HCEN. Instructions and procedures for preparing an official request for accreditation can be found in the SAM Certification Guide (11). Samples and/or templates for each document required are contained in C&A Package 2 (Reference 12) for those currently not connected to the HCEN, and in the HCEN Template for those already connected to the HCEN. IMCEN will provide guidance and assistance, as requested, in preparing the accreditation package.

The requirements for accreditation are intended to be commensurate with the system size, criticality, mode of operation, data sensitivity, and number of users. The accreditation requirements covered in this section are based on the Single Agency Manager (SAM) Certification Guide (Reference 11).

The HCEN Template has established the following policy (Reference 13):

(A) Army agencies serviced by HCEN having no system administrator rights do not need a full network accreditation.

(B) Army agencies serviced by HCEN having no ability to manage or administer their computer or network resources or configuration will be accredited as a part of the HCEN. To be accredited within the HCEN, HQDA customers must submit the following documents to the IMCEN ISSM:

(1) Checklist for Connectivity to the HCEN

(2) HCEN Logon ID Request Form

(3) Open Storage Certification Memorandum (if applicable)

(4) OISSO Appointment Letter

(5) PC Configuration and Logical Connection Layout Diagrams

(6) List and Location of Hardware and Software

(7) HCEN SOP Concurrence Memorandum

(8) Information Systems Security Inbriefing (**newly appointed OISSOs only**)

Samples and templates for each of the above are contained in C&A Package 2 (Reference 12).

(C) Army agencies serviced by the IMCEN having separate external connections or local systems administrators with the ability to manage or administer computer or network resources or configuration will need to provide an independent accreditation package. IMCEN will provide guidance and assistance in preparing the accreditation package for such HQDA customers. They must submit the following documentation to their Certifying Official:

(1) Certification Request

(2) OISSO Appointment Letter

(3) System description, including configuration diagram

(4) Security SOPs or policies, to include a contingency plan

(Guidelines for creating security policies can be found in the SAM Certification Guide [Reference 11]. The HCEN SOPs may be used as a general guideline.)

(5) Threat Analysis Worksheet

(6) Security Test and Evaluation (ST&E)

(7) Site survey information—if a site survey has been conducted by SAM-DSS.

Samples and templates for each of the above can be obtained in C&A Package 2 (Reference 12), or by contacting IMCEN: Mr. Ronald L. Greenfield, ISSM, 695-7447; or Mr. William Dugger, ISSO, 693-7070.

5.2.1 Sensitivity Determination

(A) Sensitivity determination must be accomplished using the criteria in Section 2.1 and AR 380-19, paragraph 2-2.

(B) When sensitivity has been determined, a written request must be submitted to the DAA for official designation of the sensitivity level that will meet the recommended level. This request accompanies the accreditation request.

(C) Non-sensitive designations must be authorized in the same way as sensitive designations. Each request for non-sensitive designation must be submitted to the DAA for approval and must include the rationale for arriving at this designation. After the operation is officially designated non-sensitive by the DAA, the actual accreditation is not required. However, system operations must be reviewed at 3-year intervals to ensure that the non-sensitive designation remains valid. (Note: only those portions of the accreditation that have changed need to be redone. If no changes have occurred at the

end of the 3-year period, an updated accreditation statement from the DAA may be all that that is necessary.)

5.2.2 Interim Approval

(A) A DAA may grant interim approval to operate before an operational accreditation is issued provided the provisions of AR 380-19, paragraph 3-10 are met.

(B) An interim approval may not be granted for periods longer than 90 days and only one additional 90-day extension may be granted.

5.2.3 Accreditation Statement

(A) A system cannot be legally operated without an official accreditation statement on file.

(B) The accreditation statement is signed by the DAA after review of the accreditation documentation. This statement is generated for each accreditation and reaccredidation.

(C) Through this review, the DAA states the highest sensitivity level at which information can be processed, defines the security processing mode, weighs the vulnerabilities and threats against mission requirements, and, by his or her signature, accepts the stated risks for system operation.

6. SECURITY OFFICER RESPONSIBILITIES

6.1 Purpose

The purpose of this section is to outline the Information Systems Security (ISS) responsibilities of appointed security officers, and to prescribe procedures for personnel who use automated information systems.

6.2 Scope

The policies contained herein are applicable to all agencies that use the HQDA Classified HCEN (HCEN). The HCEN is comprised of (5) servers, a switch and fiber optical cable.

6.3 Reference

AR 380-19, Information Systems Security, dated 27 February 98.

6.4 Responsibilities

(A) Information System Security Managers (ISSM) are directed as follows:

(1) Oversee the execution of the ISS training and awareness program within the command or activity.

(2) Ensure that an Information systems security officer (ISSO) is appointed for each separate AIS, group of AIS, or network as necessary.

(3) Establish an AISSP that will provide protection for all information systems and ensures all AIS and/or networks are accredited per AR 380-19.

(4) Periodically review the status of all AIS and networks to ascertain that changes have not occurred that affect security and negate the accreditation.

(5) Review threat and vulnerability assessments to enable the commander or manager to properly analyze the risks to the AIS information and determine appropriate measures to effectively manage those risks.

(6) Report security incidents and technical vulnerabilities per AR 380-19, AR 381-14, AR 380-5, and AR 381-12.

(7) Establish the scope of responsibilities for each ISSO using guidance from the ISSPM and applicable regulations.

(B) Information System Security Officers (ISSO) are directed as follows:

(1) Ensure systems are operated and maintained according to AR 380-19 and governing SOPs.

(2) Ensure managers, system administrators, and users have the appropriate security clearances, authorizations, and need-to-know.

(3) Work closely with their organization's security manager.

(4) Prepare accreditation and reaccredidation documentation for organizational systems with the assistance of the SAs and OISSOs.

(5) Include all personnel associated with AIS in system-specific and general awareness security training.

(6) Ensure procedures, instructions, guidance and SOPs concerning systems are prepared and distributed to all applicable managers, security officers and system users.

(7) Randomly review operating system audits trails for unsuccessful login/on attempts and investigate discrepancies thoroughly.

(8) Report all security incidents and violations to the Information System Security Manager (ISSM) and their security manager.

(9) Direct their SA to disseminate User IDs and passwords to users as necessary.

(10) Coordinate with other ISSOs, security managers and SAs to determine levels of access for their agency personnel.

(11) Maintain accreditation documents copies for all systems of which responsible.

(C) System Administrators (SA) are directed as follows:

(1) Ensure the networked system is properly operated and maintained.

(2) Ensure that procedures, instructions, guidance, and SOPs concerning the networked system are prepared and distributed to those concerned.

(3) Establish procedures to control access and connectivity to the network.

(4) Ensure system audit trails and system management reports are being used for internal security audits.

(5) Maintain a copy of the network accreditation documentation, and assist their ISSO in the preparation of accreditation documentation.

(D) Terminal Area Security Officers (OISSOs) are directed as follows:

(1) Implement security procedures and oversee the operation of terminal area systems.

(2) Maintain a list of individuals authorized to use automated information systems. The list will specify the level of classification users are permitted to operate systems.

(3) Ensure that automated information system users perform the duties outlined in AR 380-19 and applicable SOPs.

(4) Ensure ISSOs/SAs are advised of changes in the location of equipment, modification of system hardware and/or software, and users having access to automated information systems.

(5) Oversee the enforcement of the following:

(a) Operators use only government supplied software.

(b) Operators make a copy of mission critical data at least once every two weeks.

(c) Operators use systems for official government business only.

(d) Operators do not process classified information on a system that is connected to a network. That operators process classified information only on systems that are disconnected from networks, and are accredited to process classified information.

(e) Operators do not leave PC unattended while processing sensitive or classified information.

(f) Operators properly secure classified and sensitive data diskettes and printed output at the end of the day or when processing is complete.

(g) Operators do not eat or drink while using information systems.

(6) Inform all personnel that they are required to immediately report any actual or attempted access to any system with the intent to damage the system or commit fraud, extortion, theft, or misappropriation of funds, property, or services upon detection of the incident to their OISSO, ISSO, or security manager.

(7) Identify and explain to users the existing regulatory requirements for security of remote terminal access to other systems and procedures governing remote terminal usage.

(8) Ensure users understand the proper procedures for powering up/down their terminals, preventing disclosure of passwords when logging on/into a system and safeguarding a terminal connected to a host computer.

(9) Ensure terminals are positioned to prevent disclosure of data by unauthorized viewing.

(10) Monitor terminal usage; type of output coming back to the terminals, access to terminals, etc. The OISSO is required to be aware of what a terminal user is doing with a system

(11) Ensure display tubes are darkened or turned off at the end of the duty day. This will avoid burning of information onto the screen.

(12) Assist the ISSO/SA in providing system security.

(13) Report all practices dangerous to overall system security and all actual security violations to the ISSO/SA, as soon as recognized.

(14) The OISSO will have ready access to accreditation documentation and be familiar with the level processed and the protective requirements associated with systems operated in the terminal area. .

7. PROCEDURAL SECURITY

Procedural security measures involve a minimum of financial expenditure while producing a high level of security. The following covers ARDA II Administrator account controls and procedures, user account management, user password controls and procedures, and auditing procedures.

7.1 ARDA II Administrator Account Controls and Procedures

(A) Purpose. This section establishes controls and procedures for administrative access to the HCEN currently known as ARDA II. The source of these policies is the memorandum on Processing Information At The Classified Sensitivity Level. This SOP is effective beginning 21 October 1999 and continues until superseded or made obsolete by the ARDA II Network Management Office (IMCEN).

(B) Scope.

(1) Individuals having these levels of access have extensive, and even complete, access and permissions to the entire HCEN. Access to these permissions must be closely monitored in order to avoid unauthorized access and possible negligence.

(2) This section does not apply to administrator passwords on other networked systems that are not a member of the HCEN.

(3) Neither does this SOP apply to user accounts not having administrator privileges. User account passwords are addressed in Sections 7.2 and 7.3 and in Section V of AR 380-19.

(C) Policies:

(1) The use of the ARDA II Administrator account is granted to authorized personnel who need it to fulfill their duties. Authorized personnel include individuals employed by the Systems HCEN Network.

(2) The Administrator account will be used only when absolutely necessary; administrative tasks will otherwise be performed with the user's own (named) network account.

(3) Only the Chief, Enterprise Management Branch, and the designated government ARDA II Administrator will grant use of the Administrator account.

(4) Personnel entrusted with the password to the Administrator account will under no circumstances share it with anyone else. An ARDA II administrator will change the administrator password on a regular basis for security purposes.

(D) Procedures for Password Distribution:

(1) The password will be printed on an ARDA II Administrator Password Signature Sheet. Individuals requiring the password will sign the sheet acknowledging that they will not disclose the password to unauthorized personnel.

(2) The administrator who changes the password is responsible for (a) notifying the primary ARDA II administrator of the change and (b) ensuring that the new password is distributed as described. Once the sheet has all the required signatures, it will be given to the primary ARDA II administrator for safekeeping.

(E) Physical Security. The primary ARDA II administrator will safeguard the ARDA II Administrator Password Signature Sheet in an appropriate secured device. Only ARDA II management personnel shall have access to that device.

(F) Procedure for Password Changes:

(1) The administrator password will be changed every 90 days or when an individual who is employed in the Network Management Office terminates his position, which ever occurs first.

(2) The primary ARDA II administrator is responsible for changing the password once it reaches its maximum password age.

(3) If the Network Management Office no longer employs an individual, the Network Management Office supervisor must notify an ARDA II administrator. The administrator must change the password as soon as possible then distribute the password as defined below.

(G) Password Content:

(1) The password's minimum length is 8 characters.

(2) The password should not be a word found in the dictionary.

(3) The password can be generated at the discretion of an ARDA II administrator.

(H) Other Accounts Having Administrator Access

(1) Authorized personnel may be granted NT Administrator rights by including their NT accounts in the Administrator group. Authorized personnel include individuals employed by the Enterprise Management Branch in IMCEN who are responsible for systems within the HCEN.

(2) This access will only be granted to those authorized personnel needing it to fulfill their duties. Only the Chief, Enterprise Management Branch, and the designated government ARDA II Administrator will grant administrator rights.

(3) Personnel granted administrative rights will under no circumstances grant administrator, server operator, or account operator rights to any other user without approval by the Chief, Enterprise Management Branch, or the designated government ARDA II Administrator.

(I) Account and Server Operator Privileges

(1) Authorized personnel in ARDA II may be granted rights as Account Operator and Server Operator. Authorized personnel include individuals employed by IMCEN who are responsible for account and server maintenance within the HCEN.

(2) These privileges may also be extended to designated personnel of other HQDA Enterprise organizations whose membership exceeds 100 people. Personnel given these privileges are obligated to follow the published operating procedures for the ARDA II domain when exercising those privileges.

(3) As with the other administrative accounts, this may be done only with the explicit approval of the Chief, Enterprise Management Branch, or the designated government ARDA II Administrator.

(J) General Provisions

(1) Users with administrative access of any kind are especially cautioned to be careful in the use of their accounts. Passwords will not be shared with other personnel. Passwords will not be so simplistic that they might be easily guessed.

(2) Workstations or servers will not be left logged in and unattended; when leaving a machine, users will log out or lock the workstation.

7.2 User Account Management

(A) Purpose and Scope. This section establishes controls and procedures for creating and deleting users' accounts on the HQDA networks for which IMCEN is responsible. User accounts for Classified processing are assigned to a Classified workstation to ensure that users only access information processed on a specific workstation on a need-to-know basis.

(1) It applies only to HQDA local area networks (LANs) for which IMCEN is responsible for managing.

(2) This SOP does not apply to HQDA LANs that have their own Information Management Office performing their network management.

(3) This SOP is effective beginning 20 October 1999 and continues until superseded or made obsolete by the ARDA II Network Management Office (IMCEN).

(B) Policy:

(1) Beginning 20 October 1999, all user account management requests will be sent via the Exchange mail system.

(2) A LogOn ID Request form will be filled out electronically via e-mail. The HQDA administrators will review the form and take appropriate action.

(C) Procedure for Establishing a Classified User Account:

(1) Anyone (an information management officer [IMO], Help Desk technician, or an end user) who needs a user account to be created or modified will fill out the LogOn ID Request form. This is an electronic form also found on the ISS Intranet site.

(2) If the user account is for the HCEN, the HQDA administrator will forward the request to the Enterprise User Account Manager. The account manager will create the user account in accordance with the HCEN standards.

(3) Once the request is complete, the HQDA administrator or the HCEN User Account Manager will ensure that the action is completed.

(4) The OISSO will monitor the LogOn ID Request form for completed actions. If the request requires further action, the Help Desk will initiate a work request.

(D) Procedures for Deleting a User Account:

(1) Anyone who needs a user account to be deleted will fill out a LogOn ID Request form. This electronic form is located on the ISS Intranet site.

(2) The LogOn ID Request form requires the following information:

(a) Full name of the end user (including middle initial and rank)

(b) Agency and Office Symbol

(c) Room Number and Location

(d) Phone Number and Fax Number

(e) Signature of OISSO in the section designated for deletion of user accounts

(3) Once the LogOn ID Request form is completed and sent, the HQDA administrators will automatically receive a notification via e-mail. They will open the LogOn ID Request form and review the information. The requesting activity's point-of-contact may be notified to verify the information.

(4) The HQDA administrator will forward the request to the HCEN User Account Manager. The account manager will be deleted. The user's home directory and e-mail account will also be deleted.

(5) Once the request is complete, the HQDA administrator or the HCEN User Account Manager will modify the LogOn ID Request form to reflect that the action is complete.

(6) The Help Desk will monitor the LogOn ID Request forms for completed actions. If the request requires further action, the Help Desk will initiate a work request.

7.3 User Password Controls and Procedures

(A) Purpose and Scope. This section establishes controls and procedures for individual password accounts on ARDA II, HCEN.

(1) This SOP applies to the password assigned to all individual accounts on the ARDA II domain.

(2) This SOP is effective beginning 21 October 1999 and continues until superseded or made obsolete by the ARDA II Network Management Office (IMCEN).

(B) Policy:

(1) All passwords provided to and used by individuals are critical to the security of the system. All persons having access to passwords must be carefully instructed on password sensitivity and the meticulous care with which such critical information must be protected and the individual's personal responsibility and obligation to cooperate.

(2) Each authorized user must log on the system with a valid user ID and password. If compromise of the password is suspected, the user will immediately notify the OISSO/ISSO.

(3) Passwords must be created by the user and not be a word that can be found in the standard dictionary, contain a minimum of 8 characters in length, include at least one special character or number, and must contain letters that are a mixture of upper and lower case.

(C) Procedures for Password Changes:

(1) The user's access to an activity in the system will be controlled.

(2) The OISSO will brief all users about their responsibility regarding password security. Users will be instructed not to reveal their passwords and to use caution regarding their surrounding to prevent onlookers from compromising their passwords.

(3) Users must change their passwords once every 90 days.

7.4 Auditing

(A) Purpose and Scope. This SOP establishes controls and procedures for auditing the HQDA networks for which IMCEN is responsible.

(1) This SOP applies only to the unclassified HQDA local area networks (LANs) for which IMCEN is responsible for managing.

(2) This SOP does not apply to HQDA LANs that have their own Information Management Office performing their own network management.

(3) This SOP is effective March 27, 1998 and continues until superseded or made obsolete by the ARDA II Network Management Office.

(B) Policy:

(1) ARDA II Audit Policies. The ARDA II Audit Policy is set to the following events:

Event	Success	Failure
Logon and Logoff		X
File and Object Access	X	X
Use of User Rights	X	X
User and Group Management	X	
Security Policy Changes	X	X
Restart, Shutdown, and System	X	X
Process Tracking		X

(2) Auditing Event Logs. Upon receipt of an administrative alert, an administrator will check the event log of the server generating the alert.

(3) Administrative Alerts. Administrative alerts are event messages generated by Windows NT. These alerts warn about problems in areas such as security and access, users sessions, directory replication, printing, and server shutdown because of loss of power. Windows NT predetermines the selection of the events that trigger administrative alerts. Alert examples are a disk is near capacity or too many logon violations have occurred.

The domain controllers for ARDA II will be configured to send administrative alerts to administrators. The Server and Alerter services must be stopped and started when specifying who is to receive administrative alerts. After receiving an administrative alert, the administrator will further investigate the cause of the alert.

8. VIRUS MANAGEMENT AND INCIDENT REPORTING

(A) **Virus Management.** The use of anti-viral products provides the greatest protective countermeasure for virus protection, detection, and treatment. All systems connected to the HCEN require that IMCEN-approved anti-viral software be installed.

(B) **Incident Reporting.** If a virus is discovered, the user is authorized to use the current anti-virus software to disinfect. This must be done before sending any files out or inserting any disks. For those not technically trained, the IMCEN User Help Desk must be notified so designated technical personnel can verify the virus, determine the origin, if possible, and treat appropriately. The user will file a virus report using the ACERT Virus Reporting Form (on the following page) and forward via email to VirusReports@hqda.army.mil. The ISSO and ISSM must be notified immediately upon detection of any new viruses.

ACERT VIRUS REPORTING FORM

1. REPORTING INFORMATION

NAME (SYSADMIN, ISSM, ISSO):

PHONE: DSN or COM

E-MAIL: (if not e-mailed)

AGENCY and LOCATION:

2. VIRUS INFORMATION

NAME OF VIRUS: AV PRODUCT USED:

DATE DETECTED: DATE CLEANED:

3. COMPUTER INFORMATION

 # OF SYSTEMS INFECTED: # OF FLOPPIES INFECTED:

OPERATING SYSTEM:

4. DAMAGE REPORT

MISSION OF COMPUTER:

TYPE OF NETWORK (Type of Network - NIPRNET, etc):

IMPACT OF VIRUS ON MISSION:

☐ Total Loss ☐ Partial Loss ☐ Recovered Fully ☐ Unknown

DAMAGE (Rebuilt System, destroyed floppies, etc):

SOURCE OF INFECTION:

E-mail Floppy Other

Download (LAN, FTP, WWW, URL, etc)

LOST MANHOURS: **TOTAL # OF FILES INFECTED:**

REPORT ALL VIRUS INFECTIONS, WEEKLY, TO THE ACERT virus@liwa.belvoir.army.mil (or RCERT).

9. SECURITY TRAINING AND AWARENESS

(A) All individuals who are appointed as ISSM, ISSO and system administrators must complete an AIS security course of instruction equal to the duties assigned to them.

(B) Security training requirements for system users, including initial briefings and periodic training must consist of newcomers orientation to include:

(1) System specific training for each user

(2) Maintain ISSO/ISSM points of contact

(3) Establish password procedures

(4) Familiarity with policies to include internet, shareware, viruses, fraud waste and abuse

(C) Maintenance of training records to provide monthly reports due to SAM and paper trail of negative reports either hard copy or e-mail.

(D) Circulation of security advisories and alerts will be available by way of Systems Management Server (SMS), e-mail or web site access.

10. REFERENCES

The following is a quick reference to security-related publications. References maintained by your security representatives are italicized. The other publications, along with any not mentioned, can be checked out of the library.

1. AR 340-16 Safeguarding “For Official Use Only” Information
2. AR 340-17 Release of Information and Records from Army Files
3. AR 340-21 The Army Privacy Program
4. AR 380-4 DA Physical Security Program in the National Capital Region
5. AR 380-5 Army Information Security Program
6. AR 380-67 Army Personnel Security Program
7. AR 380-19 Information Systems Security
8. CSR 380-5 Personnel Security
9. CSR 380-5 Physical Security Procedures for Army Staff Activities in the Pentagon
10. OCSA Memo 380-5 Security
11. Single Agency Manager (Sam) Certification Guide, Single Agency Manager, 22 July 1998.
12. Templates for Certification and Accreditation to Operate within the HQDA Enterprise Network and Templates for full Certification and Accreditation to Operate within the HQDA Enterprise Network, prepared by IMCEN, September 1999.
13. Templates for Certification and Accreditation within the HQDA Classified Enterprise Network (HCEN), September 1999.